U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	NUMBER: DR 3170-001
SUBJECT: End User Workstation Configurations	DATE: May 12, 2015
	OPI: Office of the Chief Information Officer

1. PURPOSE

This Departmental Regulation (DR) establishes workstation and associated peripherals configurations to ensure and promote greater cyber protection, compatibility, and interoperability for hardware and software, and to provide consistency and standardization for the acquisition, configuration, and administration of information technology within the United States Department of Agriculture (USDA).

Application of the workstation configurations supports and implements the guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and other Federal oversight entities; facilitates the uniform application of engineering and/or technical criteria, methods, processes, and practices when evaluating and procuring new technologies; and ensures technologies align with USDA enterprise architecture business goals, processes, and meets the requirements of the following policy documents:

a. OMB Circular A-130, *Management of Federal Information Resources;*

b. *United States Government Configuration Baseline* (USGCB); and

c. The set requirements as identified in DR 3180-001, *Information Technology Standards*.

2. SCOPE

This policy applies to all USDA agencies, staff offices, employees, and contractors working for or on behalf of USDA.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This regulation supersedes DR 3170-001, *End User Workstation Standards*, dated December 12, 2007 in its entirety.

4. BACKGROUND

The *Clinger-Cohen Act of 1996* (formerly known as the *Information Technology Management Reform Act (ITMRA)*), was enacted to improve the way the federal government acquires, uses and disposes information technology (IT). Congressional mandates for IT architecture are contained in the *Clinger-Cohen Act of 1996*, 40 U.S.C. §11101 et seq. (2014) which was updated and revised by the *E-Government Act of 2002*, P.L. 107-347, 116 Stat. 2899 (2002) (codified at various sections of title 44) to reflect enterprise architecture, and OMB Circular A-130, *Management of Federal Information Resources*, requires that Federal agencies build and maintain a Technical Reference Model (TRM). The TRM has become the Application Reference Model (ARM) and the Infrastructure Reference Model (IRM) in the *Federal Enterprise Architecture Framework* (FEAF v2) that supports IT investment management and development of the enterprise architecture framework.

OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, requires Federal agencies to use voluntary consensus standards in lieu of government-unique standards, with the intention of reducing to a minimum the reliance by agencies on government-unique standards. Refer to DR3180-001, Information Technology Standards for the definition on standards.

The *Common Approach to Federal Enterprise Architecture* (Common Approach) presents an overall approach to developing and using enterprise architecture in the Federal Government by promoting increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies. Related implementation guidance from OMB is contained in various

documents, including Circulars A-11, A-130, Memoranda 97-16, 00-10, 05-22, 11-29, 12-10, and the *Digital Government Strategy*. The FEAF will help government planners implement the Common Approach.

Workstation requirements help identify IT standards that are designed to simplify, unify, or rationalize the design, interoperability, portability, and scalability of IT infrastructure components (e.g., network, hardware, systems, and application software).

5. POLICY

All USDA agencies and staff offices shall comply with the *E-Government Act of 2002*, OMB Circular A-130, OMB Circular A-119, and the FEAF v2 artifacts specifically those associated with the ARM and the IRM ensuring configurations of workstations and peripherals are maintained in accordance with these mandates.

Agencies and staff offices within USDA will be in compliance with this DR through the utilization of Departmental/Agency Blanket Purchase Agreements (BPAs) which comply with Common Criteria mandates, USGCB and are current with voluntary consensus standards.

a. Agencies and staff offices shall adhere to the following requirements when establishing compliance to departmental or agency BPAs:

(1) Establish and/or maintain uniform engineering and technical criteria;

(2) Establish and/or maintain methods, practices, and processes;

(3) Align with NIST and *Federal Information Security Management Act (FISMA),* 44 U.S.C. §3541 et seq. (2014) security requirements;

(4) Establish and/or maintain net-centric and enhanced interoperable shared services;

(5) Develop and establish technical maturity among systems and applications within budgeted limitations;

(6) Ensure alignment of investments, systems, and applications to include infrastructure;

(7) Manage the replacement of workstations and associated peripherals that are in alignment with the current, in force standards; and

(8) Promote best practices in alignment with business, performance, application, infrastructure, data, and security configurations.

b. The point of contact for this policy is the Office of the Chief Information Officer (OCIO), and the Associate Chief Information Officer (ACIO), Information Resource Management (OCIO-IRM) at enterprise.architecture@ocio.usda.gov.

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) or his/her delegated responsible staff shall:

(1) Be the final approving authority with concurrence of Agency authorities on the adoption of IT requirements and standards based on USDA requirements to ensure the security of Government networks, maximize the benefit of technology purchases, and minimize investment and operating expense; and

(2) Serve as the final reviewer and approver, with the concurrence of Agency and Staff Office authorities, of exceptions to the workstation requirements as requested by the agencies or staff offices.

b. Associate Chief Information Officer (ACIO), Information Resource Management (OCIO-IRM) shall:

(1) Develop and publish policies, regulations, and compliance requirements for the IT environment and provide channels for Agency input to and approval of those policies, regulations and compliance requirements.

(2) Provide management and oversight activities related to business, performance, application, data, infrastructure, and security configurations, including but not limited to:

(a) Reviewing and monitoring compliance with established policy requirements and standards without interfering with or impairing business functions or mission requirements; and

(b) Reporting compliance and deviations to OMB.

c. Agency and staff office CIOs shall:

(1) Implement the policies, requirements, and standards for the IT environment by:

(a) Developing internal procedures and controls in support of this policy and reviewing existing internal procedures and controls for support of this policy;

(b) Establishing effective communication between internal stakeholders and an identified Point of Contact in OCIO; and

(c) Incorporating the policies, requirements, and standards into agency and staff office capital planning and investment control (CPIC) processes.

(2) Implement and maintain business, performance, application, data, infrastructure and security configuration settings by:

(a) Documenting all deviations from standard configurations with a detailed rationale for the deviations, and request for a waiver from USDA ACIO OCIO-IRM;

(b) Requesting waivers from the ACIO OCIO-IRM that substantiates all policy exception requirements;

(c) Providing corrective action plans for the timely remediation of issues not authorized as an approved deviation;

(d) Utilizing the approved USDA products list as developed by the Standards Technical Working Group (STWG) to procure products that are aligned to DR 3180-001, the USGCB, and Common Criteria and submitting candidates for addition to the list;

(e) Procuring hardware and software from enterprise-wide BPAs when possible as they are made available; and

(f) Utilizing the Acquisition Approval Request (AAR) process prior to any IT-related procurements of $25,000 or higher with the following exception. The AAR must identify whether or not the acquisition of hardware or software being procured meets the applicable standards, identifies the BPAs to be used, and provides a detailed rationale if the product(s) and applications being procured do not meet the applicable standards.

(g) Agencies and offices will support and participate in the Enterprise Configuration and Change Management (ENTCMM) Change Advisory Boards (CAB).

d. The ENTCMM Systems (CAB) and the End User (Client) (CAB) shall:

(1) Focus on the Change and Configuration Management for USDA Enterprise-wide End User (Client) Management. Assist in the maintenance, stability, reliability and performance of the infrastructure and applications.

(2) Carefully identify, analyze, plan, manage, test and document ongoing changes at USDA Enterprise and Agency levels, to minimize the possibility of any changes negatively impacting the performance or availability of the enterprise system.

7. POLICY EXCEPTIONS

All USDA agencies and staff offices are required to conform to this policy; however, in the event that a specific policy requirement cannot be met as explicitly stated, agencies and staff offices may submit a waiver request. The waiver request shall explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memorandums to the USDA ACIO OCIO-IRM and submit the request to the Enterprise Architecture Division for review and decision via email to enterprise.architecture@ocio.usda.gov.

All OCIO organizations need to be cognizant of any waiver requests to various policies due to potential impact on network resources. All appropriate offices shall have the opportunity to comment and provide recommendations to the CIO for final decision.

Unless otherwise specified, agencies and staff offices shall review and renew approved policy waivers every fiscal year. Approved waivers shall be tracked as a plan of action and milestones (POA&M) item if remediation is needed. Approved waivers for specialized equipment with a continuing need will simply be tracked on an approved list. The ACIO OCIO-IRM shall monitor and approve waivers to this policy via the CIO.

The written exception will be in the form of a decision memorandum and will include:

a. Indication of Request for Exception;
b. Name of submitting agency or staff office;
c. Name and contact information of submitting person; and
d. Information technology description (hardware/software exception):

(1) Justification to show good cause for the exception. The request should document the justifications for the exception; and

(2) The impact of granting versus not granting the request.

-END-

APPENDIX A

REFERENCES

Circular No. A–11, *Preparation, Submission, and Execution Of The Budget*, July 2013

Common Approach to Federal Enterprise Architecture, May 2, 2012

Common Criteria IT Security Evaluation & the National Information Assurance Partnership

Common Criteria Product Compliant List

Digital Government: Building a 21st Century Platform to Better Serve The American People, May 23, 2012

DR 3180-001, *Information Technology Standards*, XXXX

E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (2002) (codified at various sections of title 44)

Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq. (2014)

OMB, Memorandum 97-16, *Information Technology Architectures*, June 18, 1997

OMB, M 00-10, *Procedures and Guidance on Implementing the Government*, April 25, 2000

OMB, M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, August 2, 2005

OMB, M-11-29, *Chief Information Officer Authorities*, August 8, 2011

OMB, M-12-10, *Implementing Portfolio Stat*, March 30, 2012

National Technology Transfer and Advancement Act of 1995; Public Law 104-113, Approved March 7, 1996

OMB, *Federal Enterprise Architecture Framework, v 2.0* (FEAF v 2.0), January 29, 2013

OMB, Circular A-130 Revised, *Management of Federal Information Resources*, February 8, 1996

OMB, Circular A-119 Revised, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, February 10, 1998

The Clinger-Cohen Act of 1996 40, U.S.C. §11101 et seq. (2014)

USDA Enterprise Roadmap 2014, March 28, 2014

United States Government Configuration Baseline (USGCB), February 19, 2010, updated January 10, 2014

APPENDIX B

ACRONYMS AND ABBREVIATIONS

AAR	Acquisition Approval Request
ACIO	Assistant Chief Information Officer
ARM	Application Reference Model
BPA	Blanket Purchase Agreement
CAB	Change Advisory Board
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
DR	Departmental Regulation
ENTCMM	Enterprise Change and Configuration Management
FEAF	Federal Enterprise Architecture Framework
FISMA	Federal Information Security Management Act
HW	Hardware
IRM	Infrastructure Reference Model
ITMRA	Information Technology Management Reform Act
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
P.L.	Public Law
POA&M	Plan Of Action and Milestones
STWG	Standards Technical Working Group
SW	Software
OCIO-IRM	Office Chief Information Officer-Information Resource Management
TRM	Technology Reference Model
U.S.C.	United States Code
USDA	United States Department of Agriculture
USGCB	United States Government Configuration Baseline

APPENDIX C

DEFINITIONS

Application Reference Model

The framework for categorizing Federal IT systems and application components help to identify opportunities for sharing, reuse, and consolidation or renegotiation of licenses. This information will often be used in conjunction with the other Reference Models to identify these opportunities.

It is a classification taxonomy used to describe the type of software applications in a particular architecture at the system, segment, agency, sector, federal, national, or international level.

Application is defined as: Software components (including Web sites, databases, email, and other supporting software) resting on Infrastructure that, when aggregated and managed, may be used to create, use, share, and store data and information to enable support of a business function.

The ARM is a categorization of different types of software, components, and interfaces. It includes software that supports or may be customized to support business. It does not include operating systems or software that is used to operate hardware (e.g., firmware) because these are contained in the IRM.

Common Criteria for Information Technology Security Evaluation

The Common Criteria permits comparability between the results of independent security evaluations. The Common Criteria does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

The Common Criteria is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

The Common Criteria is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products.

Infrastructure Reference Model

The framework and taxonomy-based reference model for categorizing IT infrastructure and the facilities that host and contain the IT infrastructure.

The IRM is a component-driven taxonomy that categorizes the network/cloud related standards and technologies to support and enable the delivery of voice, data, video, and mobile service components and capabilities.

For the purposes of IRM, Infrastructure is defined as "The generic (underlying) platform consisting of hardware (HW), software (SW), and delivery platform upon which specific/customized capabilities (solutions, applications) can be deployed."

The purpose of the IRM is to provide the foundation for classifying the technology infrastructure and the physical infrastructure that is needed to support it. The IRM supports definition of infrastructure technology items and best practice guidance to promote positive outcomes across technology implementations.